REMARKS

Claims 1-11 are Allowable

The Office has rejected claims 1-20, at pages 2-7 of the Office Action dated 5-14-08 ("Office Action"), under 35 U.S.C. §103 (a), as purportedly being unpatentable over U.S. Patent No. 6,990,591 ("Pearson"), in view of U.S. Patent No. 7,013,482 ("Krumel"). Applicants respectfully traverse the rejection.

The Office correctly admits that Pearson does not teach at least one interface mode adjustment switch as in claim 1 and points to Krumel to cure this deficiency. *See* Office Action, p. 3. The cited portions of Pearson describe an internet interface for new unit activation and details regarding setting security policy for the communication device. *See* Pearson, column 10, line 2 – column 11, line 20. The Office equates Pearson's user selectable buttons determining multiple levels of security with a controller coupled to at least one interface mode adjustment switch and selectively determining passage of material content between at least one computer and at least one interface in response to a position of at least one interface mode adjustment switch, as in claim 1. The cited user selectable buttons are part of an interface to display configuration options for selecting security policy. The configuration options limit acceptable behavior within the operation of a network, and responses to violations. *See* Pearson, column 10, lines 49-51. Pearson describes a remote monitoring center that selectively determines passage of material content. *See* Pearson, column 6, lines 41-60. Further, the user selectable buttons are not coupled to the remote monitoring center. Accordingly, the cited portions of Pearson do not teach a controller coupled to at least one interface mode adjustment switch and selectively determining passage of material content between at least one computer and at least one interface in response to a position of at least one interface mode adjustment switch, as in claim 1.

Krumel also fails to teach a controller selectively determining passage of material content between at least one computer and at least one interface in response to a position of at least one interface mode adjustment switch, as in claim 1. Specifically, in Krumel, a controller is designed for programming/loading logic to implement filtering rules in a programmable logic device. *See* Krumel, column 17, lines 50-59. In contrast to the controller of claim 1, Krumel's programmable logic device makes a judgment as to whether a packet should be passed or failed.

See Krumel, column 15 lines 40-45. The combination of Pearson and Krumel does not teach or disclose a controller that selectively determines passage of material content between at least one computer and at least one interface in response to a position of at least one interface mode adjustment switch, as in claim 1.

Further, Pearson and Krumel, alone or in combination, do not disclose at least one interface mode adjustment switch that is dedicated for use with the controller to selectively determine passage of material content, as in claim 1. The cited portions of Krumel describe various switches and several objectives of the Krumel data protection system. *See* Krumel, column 10, lines 52-63. Krumel teaches using physical switches to control the data protection system. *See* Krumel, column 18, lines 51-54. Krumel describes an update button to control updating of the programmable logic device code. *See* Krumel, Figure 9 and column 18, lines 38-41. Buttons 180 and 181 in Krumel are designed to respectively activate and deactivate filtering steps based on a configured mode of a protected computer. *See* Krumel, Figure 9 and column 18, lines 41-46. Krumel also describes a reset button 182 to control reset of the data protection system. *See* Krumel, Figure 9 and column 18, lines 46-51. None of the aforementioned switches in Krumel are dedicated for use with the controller to selectively determine passage of material content, as in claim 1.

Accordingly, the asserted combination of Pearson and Krumel fails to disclose or suggest at least one element of claim 1. Therefore, claim 1 is allowable. Claims 2-11 depend from claim 1, which Applicants have shown to be allowable. Hence, the combination of Pearson and Krumel fails to disclose at least one element of each of claims 2-11. Accordingly, claims 2-11 are also allowable, at least by virtue of their dependence from claim 1.

Further, it would not have been obvious to one having ordinary skill in the art to modify Pearson or the combination of Pearson and Krumel to arrive at the method of claim 1. Specifically, Pearson discloses a non-real time system for remotely monitoring the security status of a computer network and remotely configuring communication devices connected to a computer network using an interface that is a server-based configuration program hosted by a front end server at a remote monitoring center. *See* Pearson, column 1, lines 11-13; column 9, lines 20-34; Figure 1. Krumel teaches a firewall/data protection system filtering data packets in real time and without packet buffering. *See* Krumel Abstract. Krumel teaches reshaping an

electrical signal of a packet as a data packet comes in from one link, and then transmitting the packet down other links. *See* Krumel, column 2, lines 44-55. Krumel teaches parallel filtering, where packet data reception, filtering, and transmission are conducted simultaneously. *See* Krumel, column 3, lines 23-25. Applicants submit that combining Pearson with Krumel would result in changing Pearson's principle of operation. MPEP 2143.01 states:

"If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349" MPEP 2141.01

The Pearson system cannot be combined with Krumel's real time data protection device, because if the aforementioned systems are combined, the combination would result in changing Pearson's principle of operation.

Moreover, even if the Pearson system is combined with Krumel's data protection device, a point Applicants do not concede, the combination device can validate each received data packet either locally or remotely. If the combination device validates each received data packet locally, then each received data packet would be validated in real time. The combination device would validate each data packet before the last bit of the data packet is transmitted to an outgoing link. Since the combination device would perform data validation locally, before dispatching data packets to the remote monitoring center, such modification of the Pearson system would render the Pearson system unsatisfactory for its intended purpose of remotely monitoring and remotely configuring a communication device. *See* Pearson, column 5, lines 11-16. Similarly, if the combination device performs data validation remotely, via a remote monitoring center, then such modification would render Krumel unsatisfactory for its intended purpose of validating data packets in real time prior to dispatching the last bit of the data packet to an outgoing link. *See* Krumel, column 2, lines 47-53. Therefore, Applicants submit that there is no suggestion or motivation to make the combination device. *See In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Accordingly, Applicants respectfully submit that a *prima facie* case of obviousness does not exist based on the combination of Pearson and Krumel.

Further, the dependent claims disclose additional features not disclosed by the above cited references. For example, Pearson and Krumel do not disclose a controller contained at

least partially within at least one computer, as in claim 3. The Office asserts that this feature is taught by Pearson's Figures 4A and 4B. *See*, Office Action, p. 4. The illustrative screen shots of a user interface displaying user-selectable configuration options for selecting a security policy for the communication device and LAN are web pages, not a controller of claim 3. Further, the cited screen shots in Pearson are not contained at least partially within at least one computer. In contrast, the screen shots illustrated in Figures 4A and 4B are displayed when a user clicks on an option "modify configuration" on a main page illustrated in Figure 3. Accordingly, Pearson does not teach a controller contained at least partially within at least one computer, as in claim 3. For these additional reasons, claim 3 is allowable.

Figures 4A and 4B of Pearson are cited as teaching a controller contained at least partially within at least one interface, as in claim 4. *See* Office Action p. 4. Applicants note that the Office Action cites Figure 1 of Pearson as teaching at least one interface of claim 1. *See* Office Action, p. 3. Figure 1 depicts communication device 106 positioned between computer 102 and 108. *See* Figure 1. Applicants assume that the Office meant to equate the communication device 106 of Pearson with the at least one interface. Pearson describes the communication device 106 transmitting an alert signal to a remote monitoring center. *See* Pearson, Abstract. Figure 1 illustrates a remote monitoring center located remotely from the computer 102. Accordingly, Pearson fails to teach a controller contained at least partially within at least one interface, as in claim 4. For these additional reasons, claim 4 is allowable.

As for claim 6, the cited portions of Pearson describe different security levels. *See* Pearson, column 11, lines 8-21. However, the cited portions of Pearson do not describe a controller having a plurality of operating modes that comprise modes selected from at least two of a blocking mode, a learning mode, a partially blocking mode, and a non-blocking mode. Also, the cited portions of Pearson do not describe a learning mode, as in claim 6. Accordingly, Pearson fails to teach a controller having a plurality of modes in general and a learning mode in particular, as in claim 6. For these additional reasons, claim 6 is allowable.

The cited portions of Pearson describe the communication device activating the basic firewall, however, the cited portions of Pearson do not disclose at least one interface mode adjustment switch having a firewall activated position and a firewall deactivated position, as in claim 7. *See* Pearson column 12, lines 26-43. Accordingly, claim 7 is allowable for this additional reason.

The Office cites Pearson as teaching that at least one interface mode adjustment switch is hardware-based. *See* Office Action, p. 5. However, the cited portions of Pearson describe policy-setting buttons that are software based. *See* Pearson, column 10, lines 52-63 and Figures 4A and 4B. As discussed above, Figures 4A and 4B illustrate web pages displaying screen shots of configuration option selections. Accordingly, Pearson fails to teach at least one element of claim 10. Claim 10 is allowable for this additional reason.

Claims 12-15 are Allowable

The cited prior art references, Pearson and Krumel, do not disclose or suggest a system having an interface including "at least one interface mode adjustment switch having a plurality of operating mode selections comprising a learning mode selection ... wherein in the learning mode the controller is able to reduce the security level for tasks without requiring a user to make adjustments in said interface", as recited in claim 12.

As discussed above, Pearson discloses a system for remotely monitoring the security status of a computer network and remotely configuring communication devices connected to a computer network using an interface that is a server-based configuration program hosted by a front end server at a remote monitoring center. *See* Pearson, column 1, lines 11-13; column 9, lines 20-34; Figure 1. The Office correctly admits that Pearson does not teach at least one interface mode adjustment switch, as in claim 12. *See* Office Action, p. 3. Because Pearson does not teach at least one interface mode adjustment switch of claim 12, Pearson also does not teach at least one interface mode adjustment switch having a plurality of operating mode selections or ... wherein in the learning mode the controller is able to reduce the security level for tasks without requiring a user to make adjustments in the interface, as in claim 12.

The cited portion of Krumel describes various switches and several objectives of the Krumel data protection system. *See* Krumel, column 2, line 60 - column 3, line 20. Krumel teaches using various physical switches to control the data protection system itself in a straightforward manner. *See* Krumel, column 18, lines 51-54. Krumel teaches using physical switches to control the data protection system. *See* Krumel, column 18, lines 51-54. Krumel describes an update button to control the programmable logic device code update. *See* Krumel, Figure 9 and column 18, lines 38-41. Krumel describes buttons 180 and 181 to respectively activate and deactivate filtering steps depending on the mode of a protected computer. *See*

Krumel, Figure 9 and column 18, lines 41-46. Krumel also describes a reset button 182 to control the reset of the data protection system. *See* Krumel, Figure 9 and column 18, lines 46-51. None of the aforementioned switches are described as an interface mode adjustment switch having a plurality of operating mode selections or wherein in a learning mode the controller is able to reduce the security level for tasks without requiring a user to make adjustments in the interface, as in claim 12. Applicants respectfully submit that neither Pearson nor Krumel alone or in combination teach the aforementioned elements of claim 12.

Accordingly, the asserted combination of Pearson and Krumel fails to disclose or suggest at least one element of claim 12. Therefore, claim 12 is allowable. Claims 13-15 depend from claim 12, which Applicants have shown to be allowable. Accordingly, claims 13-15 are also allowable, at least by virtue of their dependence from claim 12.

Further, it would not have been obvious to one having ordinary skill in the art to modify Pearson or the combination of Pearson and Krumel to arrive at the method of claim 12. If the Pearson system is combined with Krumel's data protection device, a point Applicants do not concede, the combination device can validate each received data packet either locally or remotely. If the combination device validates each received data packet locally, then each received data packet would be validated in real time. The combination device would validate each data packet before the last bit of the data packet is transmitted to an outgoing link. Such modification in the Pearson system would render the Pearson system unsatisfactory for its intended purpose of remotely monitoring and remotely configuring a communication device. *See* Pearson, column 5, lines 11-16. Similarly, if the combination device performs data validation remotely, via a remote monitoring center, then such modification would render Krumel unsatisfactory for its intended purpose of validating data packets in real time prior to dispatching the last bit of the data packet to an outgoing link. *See* Krumel, column 2, lines 47-53. Therefore, Applicants submit that there is no suggestion or motivation to make the combination device. *See In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Accordingly, Applicants respectfully submit that a *prima facie* case of obviousness does not exist based on the combination of Pearson and Krumel.

Figures 4A and 4B of Pearson are cited as teaching status of at least one interface mode adjustment switch that is continuously shown on a computer desktop, as in claim 15. *See* Office

Action p. 7. As discussed above, Figures 4A and 4B illustrate web pages displaying screen shots of configuration option selections. Figures 4A and 4B are not interface mode adjustment switch status indicators that are continuously shown on said at least one computer desktop as in claim 15. In contrast, the screen shots illustrated in Figures 4A and 4B are displayed when a user clicks on an option "modify configuration" on a main page illustrated in Figure 3. Accordingly, Pearson does not teach a status of at least one interface mode adjustment switch is continuously shown on at least one computer desktop, as in claim 15. For these additional reasons claim 15 is allowable.

Claims 16-20 are Allowable

The cited references, Pearson and Krumel, either alone or in combination do not teach every element of claim 16. For example, Pearson and Krumel fail to disclose or suggest a method comprising "selecting a material content passage operating mode via at least one physical interface mode adjustment switch that is dedicated for use in selecting the material content passage operating mode", as recited in claim 16.

The Office correctly admits Pearson does not teach at least one interface mode adjustment switch, as in claim 16 and points to Krumel to cure this deficiency. *See* Office Action, p. 3. The combination of Pearson and Krumel does not teach or disclose selecting a material content passage operating mode via at least one physical interface mode adjustment switch that is dedicated for use in selecting the material content passage operating mode, as in claim 16. As correctly admitted by the Office, the communication device configuration web page is not analogous to the interface mode adjustment switch, as in claim 16.

Additionally, none of the switches described in Krumel are analogous to an interface mode adjustment switch that is dedicated for use in selecting the material content passage operating mode, as in claim 16. Krumel describes various switches and several objectives of the Krumel data protection system. *See* Krumel, column 10, lines 52-63. Krumel teaches using physical switches to control the data protection system. *See* Krumel, column 18, lines 51-54. Krumel describes an update button to control the programmable logic device code update. *See* Krumel, Figure 9 and column 18, lines 38-41. Krumel describes buttons 180 and 181 to respectively activate and deactivate filtering steps depending on the mode of a protected computer. *See* Krumel, Figure 9 and column 18, lines 41-46. Krumel also describes a reset

button 182 to control the reset of the data protection system. *See* Krumel, Figure 9 and column 18, lines 46-51. None of the aforementioned switches describe selecting a material content passage operating mode via at least one physical interface mode adjustment switch that is dedicated for use in selecting the material content passage operating mode, as in claim 16.

Accordingly, the asserted combination of Pearson and Krumel fails to disclose or suggest at least one element of claim 16. Therefore, claim 16 is allowable. Claims 17-20 depend from claim 16, which Applicants have shown to be allowable. Accordingly, claims 17-20 are also allowable, at least by virtue of their dependence from claim 16.

Further, it would not have been obvious to one having ordinary skill in the art to modify Pearson or the combination of Pearson and Krumel to arrive at the method of claim 16. Specifically, if the Pearson system is combined with Krumel's data protection device, a point Applicants do not concede, the combination device can validate each received data packet either locally or remotely. If the combination device validates each received data packet locally, then each received data packet would be validated in real time. The combination device would validate each data packet before the last bit of the data packet is transmitted to an outgoing link. Such modification in the Pearson system would render the Pearson system unsatisfactory for its intended purpose of remotely monitoring and remotely configuring a communication device. *See* Pearson, column 5, lines 11-16. Similarly, if the combination device performs data validation remotely, via a remote monitoring center, then such modification would render Krumel unsatisfactory for its intended purpose of validating data packets in real time prior to dispatching the last bit of the data packet to an outgoing link. *See* Krumel, column 2, lines 47-53. Therefore, Applicants submit that there is no suggestion or motivation to make the combination device. *See In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Accordingly, Applicants respectfully submit that a *prima facie* case of obviousness does not exist based on the combination of Pearson and Krumel.

Claims 17-20 depend from claim 16, which Applicants have shown to be allowable. Accordingly, claims 17-20 are also allowable, at least by virtue of their dependence from claim 16.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the cited portions of the cited references as applied in the Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the rejections, as well as an indication of the allowability of each of the pending claims.

Any changes to the claims in this amendment, which have not been specifically noted to overcome a rejection based upon the cited art, should be considered to have been made for a purpose unrelated to patentability and no estoppel should be deemed to attach thereto.

The Examiner is invited to contact the undersigned attorney at the telephone number listed below if such a call would in any way facilitate allowance of this application.

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

8-8-2008
Date

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicants
TOLER LAW GROUP, INTELLECTUAL PROPERTIES
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)